(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US01/09631

(22) International Filing Date: 26 March 2001 (26.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/536.203   27 March 2000 (27.03.2000)   US

(71) Applicant: SECURIT-E-DOC, INC. [US/US]; 1689 Forum Place. West Palm Beach. FL. 33401 (US).

(72) Inventor: BARRON, Robert, H.; 1025 Morse Blvd.. Singer Island. FL 33404 (US).

(74) Agent: SLAVIN, Michael; McHale & Slavin. P.A.. 4440 PGA Blvd.. Suite 402. Palm Beach Gardens. FL 33410 (US).

(81) Designated States (national): AE. AG. AL.. AM. AT. AU. AZ. BA. BB. BG. BR. BY. CA. CH. CN. CU. CZ. DE. DK. DM. DZ. EE. ES. FI. GB. GD. GE. GH. GM. HR. HU. ID. IL.. IN. IS. JP. KE. KG. KP. KR. KZ. LC. LK. LR. LS. LT. LU. LV. MA. MD. MG. MK. MN. MW. MX. NO. NZ. PL. PT. RO. RU. SD. SE. SG. SL. SK. SI.. TJ. TM. TR. TT. TZ. UA. UG. UZ. VN. YU. ZA. ZW.

(84) Designated States (regional): ARIPO patent (GH. GM. KE. LS. MW. MZ. SD. SL.. SZ. TZ. UG. ZW.). Eurasian patent (AM. AZ. BY. KG. KZ. MD. RU. TJ. TM). European patent (AT. BE. CH. CY. DE. DK. ES. FI. FR. GB. GR. IE. IT. LU. MC. NL. PT. SE. TR). OAPI patent (BF. BJ. CF. CG. CI. CM. GA. GN. GW. ML. MR. NE. SN. TD. TG).

Published:
—   without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations. refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD, APPARATUS, AND SYSTEM FOR SECURE DATA TRANSPORT

(57) Abstract: A platform allowing for the secure file transfer from one location to another (internet or intranet) with virtually impregnable encryption. secure data storage. and a simple web-based user interface. A user accesses the system by a data-base authentication system requiring user name and password. The program residing on the server then generates an encryption sequence. A temporary file is created on the users' machine upon which the user uploads the information to be sent. The information is automatically encrypted by the program and transferred to the server and the user's temporary file deleted. The information is securely stored in the program on the server until the recipient downloads it. The recipient also accesses the server by a user name and password. The program generates a decryption program. The recipients machine receives the applet program to decrypt the file and a copy of the encrypted file. After decryption is complete. the program saves the files to a specified recipient folder. and can be automatically deleted or archived.

1   **METHOD, APPARATUS, AND SYSTEM FOR SECURE DATA TRANSPORT**

2   FIELD OF THE INVENTION

3   This invention relates generally to the field of data

4   transmission over computer networks and more particularly

5   to a universally adaptable server-side software system for

6   an automatically encrypted and decrypted, password

7   controlled secure transfer of data from a source host to a

8   destination host across any internetwork.

9

10   BACKGROUND OF THE INVENTION

11   In recent years, the widespread adoption of public

12   and private networks has modernized the manner is which

13   organizations communicate and conduct business. Advanced

14   networks provide an attractive medium for communication

15   and commerce because of their global reach, accessability,

16   use of open standards, and ability to permit interactions

17   on a concurrent basis. Additionally, networks allow

18   businesses a user-friendly, low cost way to conduct a wide

19   variety of commercial functions electronically.

20   A computer network is basically a collection of

21   computers that are physically and logically connected

22   together to exchange data or "information." The network

23   may be local area network, connected by short segments of

24   ethernet or to the same network hub, or wide area network,

25   separated by a considerable distance. An internetwork is

26   a network of computer networks, of which the Internet is

27   commonly acknowledged as the largest.

28   The Internet is based on standard protocols that

29   allow computers to communicate with each other even if

30   using different software vendors, thus allowing anyone

31   with a computer easy accessability to everything else

32   connected to the Internet world wide. As a result of this

33   global access, it is becoming increasingly useful for

34   businesses and individuals to transmit information via

35   networks and internetworks from one site to another.

1   The interconnected computers exchange information
2   using various services, for example, the World Wide Web
3   (WWW)and electronic mail.. The WWW created a way for
4   computers in various locations to display text that
5   contained links to other files.. The WWW service allows a
6   server computer system (Web server or Web site) to send
7   graphical Web pages of information to a remote client
8   computer system. The remote client computer system can
9   then display the Web pages.
10   In a standard e-mail system, a user's computer is
11 connected to a provider of Internet services, and the
12 user's computer provides an e-mail password when polling
13 the provider's computer for new mail. The mail resides on
14 the provider's computer in plain text form where it can be
15 read by anyone. In both examples, the information, if
16 unsecured, is replicated at many sites in the process of
17 being transmitted to a destination site and thereby is
18 made available to the public.
19   Organizations are increasingly utilizing these
20 networks, to improve customer service and streamline
21 business communication through applications such as e-
22 mail, messaging, remote access, intranet based
23 applications, on-line support and supply chain
24 applications. The very openness and accessibility that
25 has stimulated the use of public and private networks has
26 also driven the need for network security.
27   Presently, to provide for a secure transfer of
28 information, it may be encrypted at the sending host's end
29 and decrypted at the receiver's end. Encryption
30 algorithms transform written words and other kinds of
31 messages so that they are unintelligible to unauthorized
32 recipients. An authorized recipient can then transform
33 the words or messages back into a message that is
34 perfectly understandable. Currently, there are two basic
35 kinds of encryption algorithms (1) symmetric key

1   algorithms and (2) public key algorithms.

2   Symmetric (or private) key algorithms use the same

3   key to encrypt and decrypt the message. Generally, they

4   are faster and easier to implement than public keys.

5   However, for two parties to securely exchange information,

6   those parties must first securely exchange an encryption

7   key. Examples of symmetric key algorithms include DES,

8   DESX, Triple-DES, Blowfish, IDEA, RC2, RC4, and RC5.

9   Public key algorithms use one key (public key) to

10   encrypt the message and another key (private key) to

11   encrypt it. The public key is made public and is used by

12   the sender to encrypt a message sent to the owner of the

13   public key then the message can only be decrypted by the

14   person with the private key. Unfortunately, public keys

15   are very slow, require authentication, and do not work

16   well with large files.

17   A third type of system is a hybrid of the public and

18   private systems. The slower public key cryptography is

19   used to exchange a random session key, which is then used

20   as the basis of a symmetric (private) key algorithm. The

21   session key is used only for a single encryption session

22   and is then discarded. Nearly all practical public key

23   cryptography implementations in use today are actually

24   hybrid systems.

25   Finally, message digest functions are used in

26   conjunction with public key cryptography. A message

27   digest function generates a unique pattern of bits for a

28   given input. The digest distills the information

29   contained in a file into a single large number, typically

30   128 and 256 bits in length. The digest value is computed

31   in such a way that finding an input that will exactly

32   generate a given digest is computationally infeasible.

33   Message digest algorithms are not used for encryption

34   or decryption but for creation of digital signatures,

35   messages authentication codes (MAC), and the creation of

1   encryption keys from passphrases. For example, Pretty

2   Good Privacy (PGP) uses message digests to transform a

3   passphrase provided by a user in to an encryption key that

4   is used for symmetric encryption. (PGP uses symmetric

5   encryption for its "conventional encryption" function as

6   well as to encrypt the user's private key). A few digest

7   in use are HMAC, MD2, MD4, MD5, SHA, and SHA-1.

8   Working cryptographic systems can be divided into two

9   categories; (1) programs and protocols that are used for

10   encryption of e-mail messages such as PGP and S/MIME and

11   (2) cryptographic systems used for providing

12   confidentiality, authentication, integrity, and

13   nonrepudiation in a network environment. The latter

14   requires real-time interplay between a client and a server

15   to work properly. Examples include Secure Socket Layer

16   (SSL) a general-purpose cryptographic protocol that can be

17   used with any TCP/IP service and PCT a transport layer

18   security protocol for use with TCP/IP service, PCT, S-

19   HTTP, SET, Cybercash, DNSSEC, Ipsec, IPv6, Kerberos, and

20   SSH.

21   Although the present means of securing the electric

22   transfer of information provides a level of security, the

23   security provided can be easily breached. Symmetric

24   encryption algorithms are vulnerable to attack by (1) key

25   search or brute force attacks, (2) cryptanalysis, and (3)

26   systems-based attacks. First, in a key search, the cracker

27   simply tries every possible key, one after another, until

28   the he/she is allowed into the system or the ciphertext is

29   decrypted. There is no way to defend against this but a

30   128 bit key is highly resistant because of the large

31   number of possible keys to be tried.

32   Second, in cryptanalysis, the algorithm can be

33   defeated by using a combination of sophisticated

34   mathematics and computer power. Many encrypted messages

35   can be deciphered without knowing the key. Finally, the

1   cryptographic system itself is attacked without actually

2   attacking the algorithm.

3   Public key algorithms are theoretically easier to

4   attack then symmetric key algorithms because the attacker

5   has a copy of the public key that was used to encrypt the

6   message. Also, the message presumable identifies which

7   public key encryption algorithm was used to encrypt the

8   message. These attacks are (1) factoring attacks and (2)

9   algorithmic attacks. First, factoring attacks attempt to

10 derive a private key from its corresponding public key.

11 This attack can be performed by factoring a number that is

12 associated with the public key.

13   Second, an algorithm attack consists of finding a

14 fundamental flaw or weakness in the mathematical problem

15 on which the encryption system is based. Although not

16 often done, it has been accomplished.

17   Message digest functions can be attacked by (1)

18 finding two messages-any two messages-that have the same

19 message digest and (2) given a particular message, find a

20 second message that has the same message digest code.

21   Thus, what is needed is a system for securing the

22 electronic transfer of information that circumvents

23 decryption. Also, needed is one system that can be used

24 for both e-mail and internet security. Finally, needed is

25 a widely available, user-friendly system for securing

26 electronic transfer and storage of information.

27

28 SUMMARY OF THE INVENTION

29   The present invention provides a universally

30 adaptable server-side software system designed to

31 administrate access and facilitate virtually impregnable

32 security for the delivery, storage, and sharing of

33 documents and files utilizing any compatible network as a

34 secure communications forum.

35   In general, the instant invention is a method and

1   apparatus for encrypting data with a either a random
2   automatic mode of encryption, and a client selected
3   private key, that does not travel with the document. The
4   method and apparatus, writes the encryption algorithm
5   creating a packaged application. The encryption program
6   generates random sequences or encryption algorithms, with
7   respect to time sensitivity, to be used in the packaged
8   application that it creates. No two algorithms will ever
9   be the same.
10   In the basic embodiment, the client accesses the
11   server using a data-base authentication system requiring
12   User name and Password. Once access is granted, the
13   packaged application is sent to the client machine as a
14   temporary file to encrypt the files being sent or uploaded
15   to the server. The application package breaks the files
16   down into binary form, reads the binary form, and then
17   rewrites the data to the temporary file it created. On a
18   binary level, the code is rewritten and saved for transfer
19   in a file format only decodable by the end recipient.
20   Once this process is complete, the application packet then
21   sends the encrypted data to the server via SSL protocol
22   connection.
23   The data resides on the server waiting for an
24   intended recipient to download and unlock it. When file
25   retrieval is requested, the server authenticates the user
26   and password via a log-on system. Once access is granted,
27   the server generates a new application packet designed to
28   decrypt the file being requested, based on the original
29   encryption algorithm. The server retrieves its original
30   entry, sets into motion the sequence of creating a
31   decryption program, saves the generated program, and then
32   sends the application packet to the requesting client
33   machine.
34   The client machine receives the application packet to
35   decrypt the file from the server and a copy of the file to

1   be decrypted is downloaded. The application program now
2   runs the calculations it needs to decrypt the data with
3   the sequence it was given. The application program opens
4   the file, reads the binary data, and writes the data to a
5   new temporary file created for its reception. When the
6   file is decrypted, the program saves the file to a folder
7   specified by the recipient and then deletes itself
8   providing a secure transfer. Upon completion of the
9   transfer, the original encrypted file located on the
10 server can be deleted or retained archival.
11   Accordingly, it is an objective of the instant
12 invention to provide a method and apparatus that provides
13 secure electronic transfer of information by using a
14 random and automatic mode of encryption wherein no two
15 algorithms are ever repeated.
16   Still another objective of the instant invention to
17 provide a method and apparatus that allows for secure data
18 transportation that encrypts at the 128 bit level,
19 transports and stores data encrypted, and decrypted only
20 to an authorized user.
21   A further objective of the instant invention to
22 provide a basic level of security wherein data is
23 transported via an SSL protocol and automatically
24 encrypted. In this mode only authorized user on a network
25 can decrypt data for review or modification. Separately
26 and in addition, a secure e-mail notification is
27 dispatched to the intended recipient(s) to inform them of
28 secure data waiting for retrieval.
29   Another objective of the instant invention to provide
30 a heightened level of security wherein a private and
31 secondary key or digital file lock can be employed
32 providing a unique secondary data lock.
33   Still another objective of the instant invention to
34 provide a client-side locking device or biometric
35 interface. In such a locking device, a retinal scanner,

1 finger print scanner., smart card reader or the like anc be

2 implemented in order to send or retrieve information.

3   Yet another objective of the instant invention is to

4 provide virtually impregnable security for the delivery,

5 storage, and sharing of documents and files utilizing any

6 compatible network as a secure communications forum.

7   Other objects and advantages of this invention will

8 become apparent from the following description taken in

9 conjunction with the accompanying drawings wherein are set

10 forth, by way of illustration and example, certain

11 embodiments of this invention. The drawings constitute a

12 part of this specification and include exemplary

13 embodiments of the present invention and illustrate

14 various objects and features thereof.

15

16 BRIEF DESCRIPTION OF THE FIGURES

17   Figure 1 is a block diagram of the client file

18 encryption transfer request of the instant invention;

19   Figure 2 is a block diagram of the encryption

20 transfer;

21   Figure 3 is a block diagram of the recipient file

22 request; and

23   Figure 4 is a block diagram of the decryption

24 transfer.

25

26 DETAILED DESCRIPTION OF THE INVENTION

27   Although the invention will be described in terms of

28 a specific embodiment, it will be readily apparent to

29 those skilled in this art that various modifications,

30 rearrangements, and substitutions can be made without

31 departing from the spirit of the invention. The scope of

32 the invention is defined by the claims appended hereto.

33   Now, referring to Fig. 1, shown is flow chart

34 depicting the steps required for encrypting data allowing

35 for secure transfer of electronic data. A client 10 opens

1   a web browser and accesses a qualified server 12 therein

2   requesting data transfer. The server 12 provides login

3   account qualifier data requiring either user name and a

4   password 14 or a biometric interface 16 such as a retinal

5   scanner, finger print scanner, smart card reader and the

6   like for the purpose of seeking data-base authentication

7   18.   If login fails, the user has three attempts 20

8   before the account is locked 22 and the administrator and

9   the account holder 24 is alerted. Upon a successful login

10 26, a transfer request 28 is sent to the control program

11 on the server to open a transfer information page inquiry

12 page.

13   Referring now to Figure 2, when data is to be

14 transferred 30, an applet is compiled on the server and

15 sent to the client 32. The applet is a temporary file

16 allowing the client to select 34 the data files that are

17 to be transferred. The user adds the file(s) to be

18 transferred to the application window 46. If the user

19 account allows, the client has the option of entering via

20 the keyboard, a secondary security key 36. It should be

21 noted that even if two separate people encrypted the exact

22 same file with the same key, they will have encrypted two

23 uniquely different sequences. If one attempts to "crack"

24 the application sequence, they would not be able to

25 decrypt it because each applet is embedded with a unique

26 encryption sequence. The encryption sequence generated is

27 added to the applet template and compiled 38 and

28 transferred to the server 40 with notification sent to the

29 recipient 42.

30   The applet breaks the code of the files down into its

31 binary form during execution. It reads the binary data

32 and then rewrites the data to the temporary file that was

33 previously created. The running program changes the

34 entire code sequence of the client file to a randomly

1   generated sequence specified by the particular and

2   customized applet.. The sequence is also designed to

3   replace every other matching bit of binary code with a

4   unique string.. Thus, with this method, an "a", for

5   example, will never be represented twice in the same file

6   structure. This is designed to deter the common method of

7   cracking encrypted code by repeated or pattern data. On

8   a binary level, the code is rewritten and saved for

9   transfer in a file format only decodable by the recipient.

10   The applet then sends the encrypted data to the server via

11   SSL protocol. Once the transfer is complete, the applet

12   deletes any trace of the file encrypted. With the

13   destruction of the applet, no two applications are ever

14   the same because each application contains it's own

15   encryption sequence that cannot be replicated.

16   The encrypted data resides on the server 12 waiting

17   for an intended recipient to download and unlock it. This

18   creates the ability to maintain completely encrypted and

19   secure data archives. When file retrieval is requested by

20   a recipient, the server then accesses the original record

21   information of the sequence or algorithm that it

22   originally gave to the applet that the server created to

23   encrypt the file.

24   Now referring to Fig. 3, shown is the flow chart

25   depicting the steps for decrypting data for a secure

26   receipt of electronic data. A recipient 50 opens a web

27   browser and accesses a qualified server 12 therein

28   requesting data transfer. The server 12 provides login

29   account qualifier data requiring either user name and a

30   password 52 or a biometric interface 54 such as a retinal

31   scanner, finger print scanner, smart card reader and the

32   like for the purpose of seeking data-base authentication

33   56. If login fails, the user has three attempts 58

34   before the account is locked 60 and the administrator and

35   the account holder 62 is alerted.

-11-

1   If the login is successful, the server 12 depicts

2   those files available to the recipient 66.. The recipient

3   chooses which file to retrieve and the server generates a

4   new applet designed to decrypt the file requested 69,

5   based on the original encryption sequence. The file is

6   retrieved 70 and stored in a temporary file.. The program

7   now prompts the user for any secondary key 71 that was

8   originally entered by the sender. Once the key sets the

9   sequence, the applet calculates the sequence that was

10   originally written on the fly. The applet resumes

11   decryption with the new sequence of the temporary file

12   wherein decryption is executed 72 and the decrypted file

13   saved to a selection location. When the data decryption

14   is complete, the program saves the file 73 with original

15   extensions, to a folder specified by the recipient. Then

16   the applet deletes itself 74 and any data related to the

17   secure transfer. Upon completion of the transfer and

18   decryption process, the original encrypted file located on

19   the server can be triggered to be automatically deleted or

20   retained for manual deletion.

21   It is to be understood that while a certain form of

22   the invention is illustrated, it is not to be limited to

23   the specific form or arrangement of parts herein described

24   and shown. It will be apparent to those skilled in the

25   art that various changes may be made without departing

26   from the scope of the invention and the invention is not

27   to be considered limited to what is shown and described in

28   the specification and drawings.

29

30

31

32

33

34

CLAIMS

What is claimed is::

Claim 1. A method of encrypting data for secure transfer and storage of electronic data comprising the steps of:

accessing a conventional web browser;

logging onto a qualified server and providing account qualifier data;

reading a transfer information inquiry page upon verification of account qualifier;

obtaining a first applet compiled on said server in response to said inquiry page, said first applet used to create a temporary file for the upload of data;

submitting a file for encryption to said applet;

encrypting said file and forming an encrypted data packet;

forwarding said data packet to said qualified server for storage;

providing a means for decrypting said encrypted data packet.

Claim 2. The method according to claim 1 wherein said account qualifier is a user name and password.

Claim 3. The method according to claim 1 wherein said account qualifier is a smart card reader.

Claim 4. The method according to claim 1 wherein said account qualifier is a biometric interface.

Claim 5. The method according to claim 4 wherein said biometric interface is a retinal scanner.

1   Claim 6. The method according to claim 4 wherein
2   said biometric interface is a finger print scanner.
3
4   Claim 7. The method according to claim 1 including
5   the step of entering a secondary security key to said
6   applet.
7
8   Claim 8. The method according to claim 7, wherein
9   said secondary key is a digital file lock.
10
11   Claim 9. The method according to claim 1 including
12   the step of destroying said first applet.
13
14   Claim 10. The method according to claim 1 wherein a
15   recipient is notified of an encrypted data file by an e-
16   mail message sent via the open SSL protocol upon
17   submittal of said data packet to said server.
18
19   Claim 11. The method according to claim 1 wherein
20   said means for decrypting said encrypted data packet
21   comprising the steps of:
22   accessing a conventional web browser;
23   logging onto a qualified server and providing account
24   qualifier data;
25   reading a transfer information inquiry page upon
26   verification of account qualifier;
27   obtaining a second applet compiled on said server in
28   response to said inquiry page, said second applet used to
29   create a temporary file for the download of data;
30   submitting a file for decryption to said second
31   applet;
32   decrypting said file.
33
34   Claim 12. The method according to claim 10 wherein
35   said second applet is destroyed.

1

2   Claim 13.   The method according to claim 1 wherein

3   said account qualifier is compared against a stored

4   database.

5

6   Claim 14.   The method according to claim 1 said

7   encrypting of said file occurs during a transfer to said

8   server.

9

10   Claim 15. A method of encrypting data for secure

11   transfer and storage of electronic data comprising the

12   steps of:

13   accessing a conventional web browser;

14   logging onto a qualified server and providing account

15   qualifier data;

16   reading a transfer information inquiry page upon

17   verification of account qualifier;

18   obtaining a first applet compiled on said server in

19   response to said inquiry page, said first applet used to

20   create a temporary file for the upload of data;

21   submitting a file for encryption to said applet;

22   encrypting said file and forming an encrypted data

23   packet;

24   forwarding said data packet to said qualified server

25   for storage and destroying said first applet;

26   obtaining a second applet compiled on said server in

27   response to said inquiry page, said second applet used to

28   create a temporary file for the download of said encrypted

29   data;

30   decrypting said file and destroying said second

31   applet.

32

33   Claim 16.   The method according to claim 15 wherein

34   said account qualifier is a user name and password.

35

1   Claim 17.. The method according to claim 15 wherein
2   .said account qualifier is a .smart card reader..
3
4   · Claim 18.. The method according to claim 15 wherein
5   said account qualifier is a biometric interface..
6
7   Claim 19. The method according to claim 18 wherein
8   said biometric interface is a retinal scanner.
9
10   Claim 20. The method according to claim 18 wherein ·
11 said biometric interface is a finger print scanner.
12
13   Claim 21. The method according to claim 15 including
14 the step of entering a secondary security key to said
15 applet.
16
17   Claim 22. The method according to claim 21, wherein
18 said secondary key is a digital file lock.
19
20   Claim 23. The method according to claim 15 wherein a
21 recipient is notified of an encrypted data file by an e-
22 mail message sent by SSL protocol upon submittal of said
23 data packet to said server.
24
25   Claim 24. A system for secure transfer, storage and
26 access of electronic data comprising;
27   a software system program residing on a server having
28 a login entry sequence, means for generating a program
29 for encrypting data selected by a sender to create a first
30 applet, said first applet used to create a temporary file
31 on said sender's computer for the upload of data to be
32 transferred forming an encrypted data file, means for
33 transporting and storing of said encrypted data file,
34 means for generating a second applet to retrieve and
35

1   decrypt said data file, said second applet allowing for

2   the downloading and decryption of said data file.

3

4   Claim 25.   The system according to claim 24, wherein

5   said applets are controlled by a user name and password.

6

7   Claim 26.   The system according to claim 24, wherein

8   said sender selects a secondary private key to layer said

9   encryption.

10

11   Claim 27.   The system according to claim 26, wherein

12   said secondary key is a digital file lock.

13

14   Claim 28.   The system according to claim 26, wherein

15   said secondary key biometric interface.

16

17   Claim 29.   The system according to claim 24 wherein

18   the recipient is notified of an encrypted data file by an

19   e-mail message generated by said system and directed to

20   said recipient.

21

22   Claim 30.   The system according to claim 29 wherein

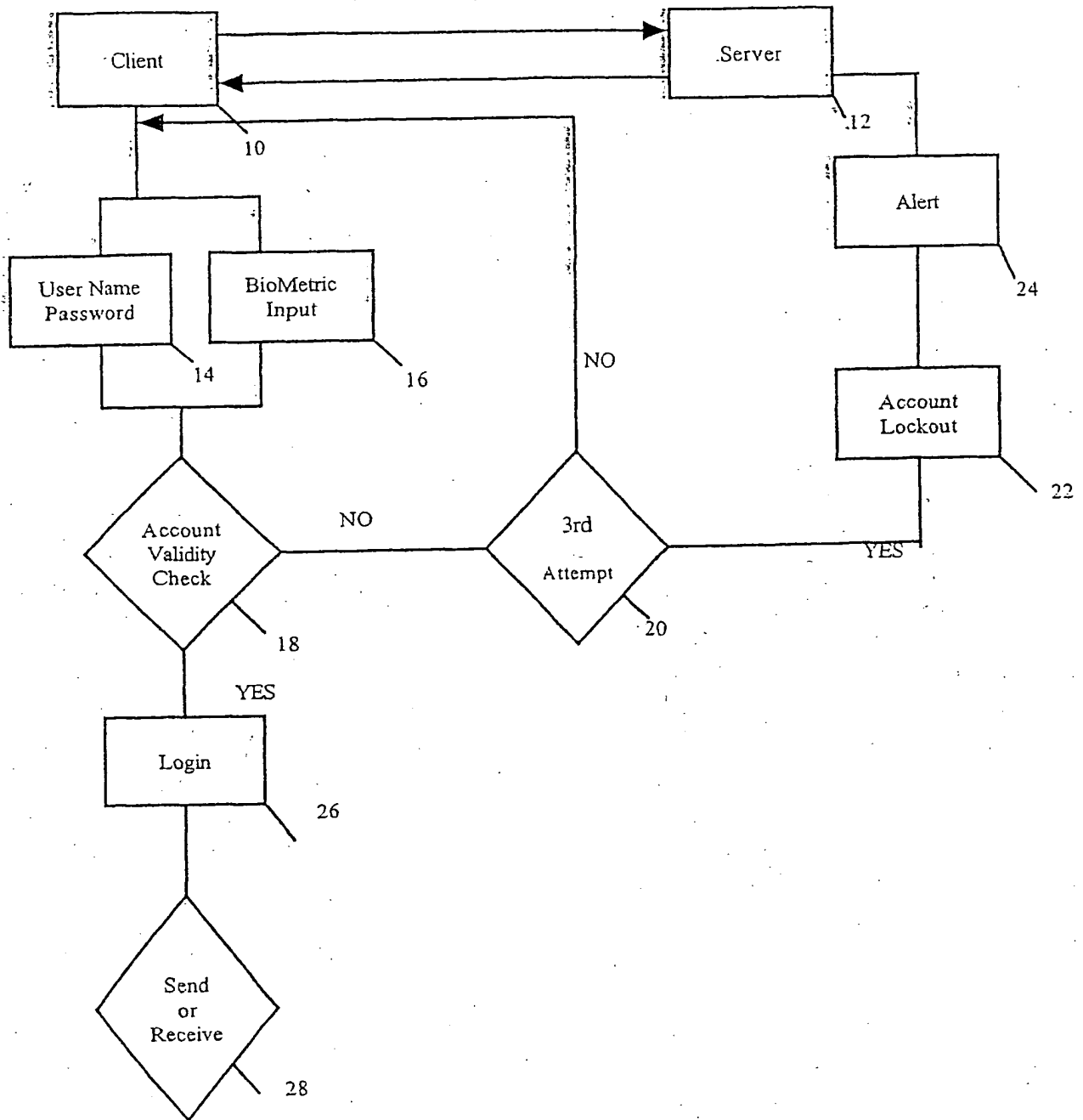23   said e-mail is sent by SSL protocol.

24

25

Fig 1

Transfer
Request
30

Applet Compiled
on Server and
delivered to Client
32

Selection
of Files
34

Secondary
Key

Encryption
of Data
38

Encrypted
Data Sent
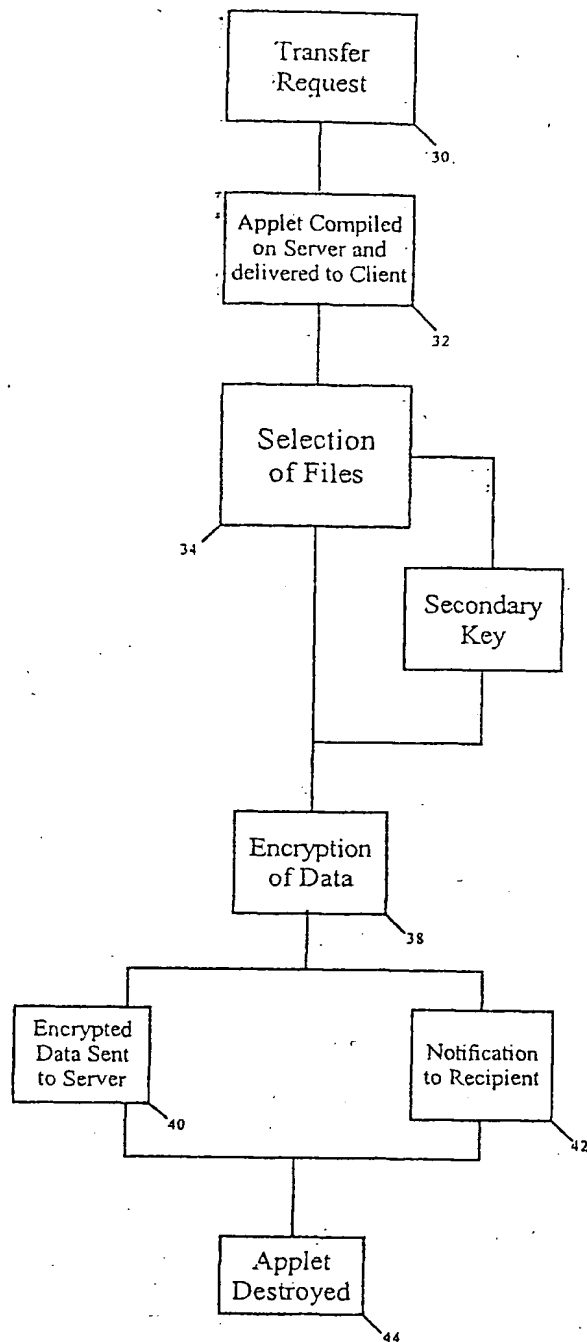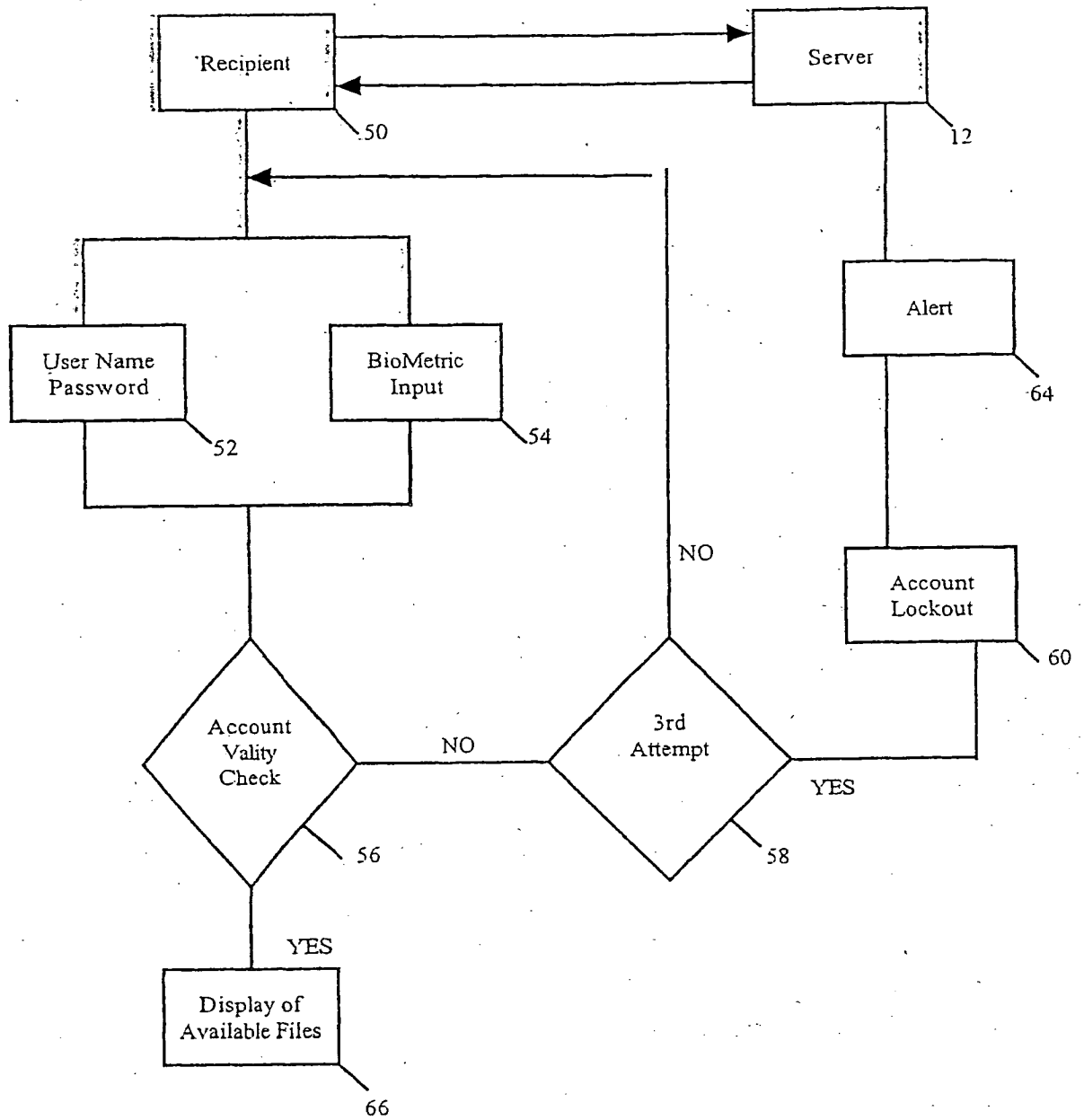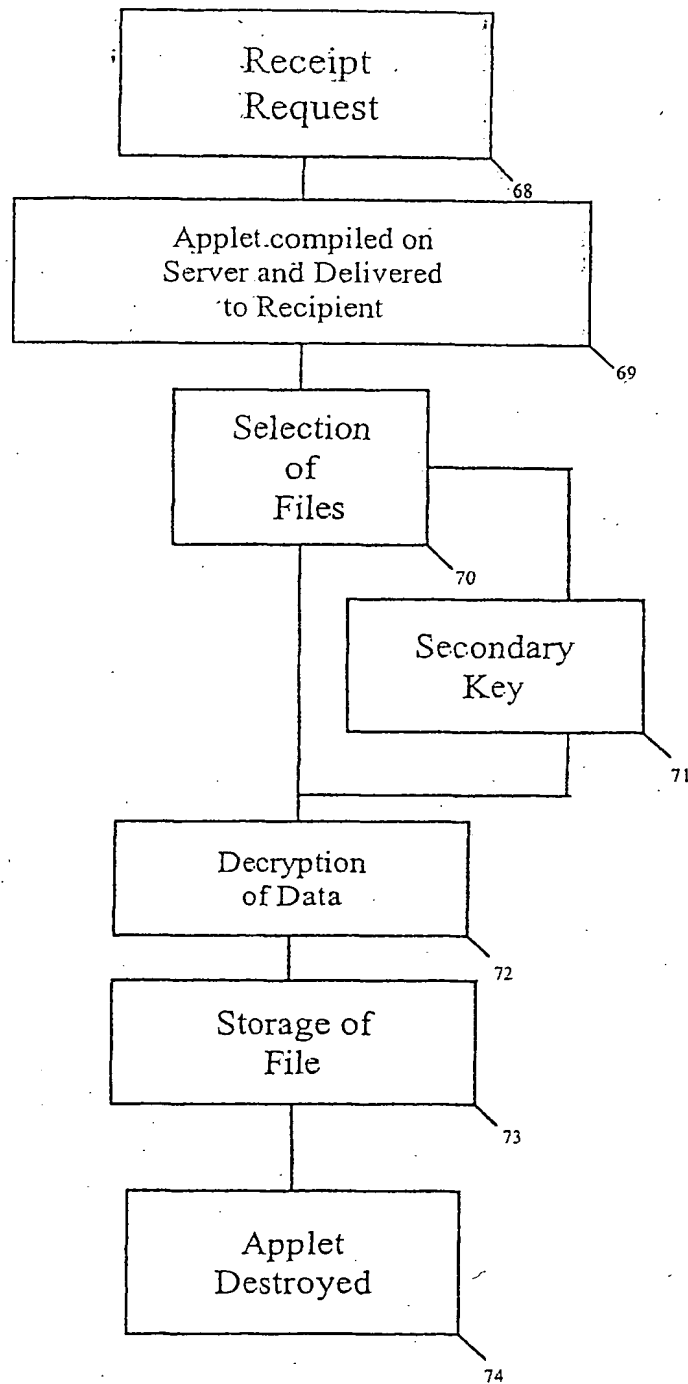to Server
40

Notification
to Recipient
42

Applet
Destroyed
44

Fig 2

Fig 3

Fig 4.

This Page Blank (uspto)